

AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT APPLICATION

I, Joshua Borges, a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 130 Gross Neck Road, Waldoboro, Maine (hereafter "Premises"), further described in Attachment A, for the things described in Attachment B.
2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for federal criminal offenses. I also am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.
3. I have been an FBI TFO since May 14, 2018. I am also a Supervisor with the U.S. Department of Homeland Security, U.S. Customs and Border Protection (CBP), Office of Field Operations. I have been employed with CBP since April 27, 2009.
4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and records related to this investigation, and information gained through my training and experience.
5. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe, and I do believe, that violations of Title 18, United States Code, Section 875(c)

(interstate transmission of threat to injure) have occurred. I submit that there is also probable cause to search the location described in Attachment A for evidence of this crime, further described in Attachment B.

PROBABLE CAUSE

Report of Threat on Twitter

6. On June 1, 2019, the FBI's National Threat Operations Center (NTOC), which receives tips regarding potential criminal activity, received an online tip from an individual in Kentucky regarding a threat that had been made via Twitter. According to the individual who submitted the tip, a Twitter user with the user name troy41581612 had tweeted that he planned to carry out a mass shooting at a Boston high school in September or October. The individual provided a link to the tweet in question.

7. A review of the tweet in question confirmed that on June 1, 2019, at 12:02 p.m., the Twitter user Troy41581612 tweeted, "I just want to let you all know that I'm planning to shoot up a Boston high school. I'm 25 year old with autism spectrum disorder and live with my parents." In what appeared to be replies to his own initial tweet, the same user stated, "I'm tired of being bullied all my life," and "My plan is to shoot up the school either September or October."

8. Later on June 1, FBI personnel sent an emergency disclosure request to Twitter, requesting subscriber information for the account Troy41581612. Information provided by Twitter in response to the request showed that the account's user provided the email address troyglidden@gmail.com when the account was opened, and that the account had been opened using IP address 98.11.137.132. Publicly available, open-source information indicated that the IP address was assigned to Charter Communications.

9. Also on June 1, FBI personnel sent an emergency disclosure request to Charter Communications. In response to the request, Charter reported that the IP address in question was assigned to Karen Glidden at the Premises.

Reports of Threat on Yahoo! Answers

10. On June 2, 2019, an individual in Illinois submitted a tip to the NTOC regarding a threat that someone had posted to the question-and-answer internet site Yahoo! Answers. The individual stated that someone with the user name “troy” had written that he was planning to shoot up a Boston high school in September or October. The individual also stated that “troy” had been recently posting threatening questions and comments involving guns and homemade bombs, and had posted about sympathizing with the individual who committed the Newtown, Connecticut school shooting. The individual suspected that “troy” was just an internet troll trying to create trouble, “but with all of the stuff that has happened over the last 10 years, why ignore it.”

11. On June 3, 2019, the Verizon Media E-Crime Investigations Team independently provided information on the same Yahoo! Answers user to the Waldoboro Police Department.¹ Verizon reported that the user appeared to be a 25-year-old male living in or around Waldoboro. Verizon also reported that the user had made multiple comments in Yahoo! Answers stating that he had autism spectrum disorder and discussing his intent to shoot up a Boston high school or commit other violent acts.

12. Verizon also provided more detail regarding the user’s posts on Yahoo! Answers. They included the following postings, which were flagged by moderators because of their concerning nature:

¹ Verizon Communications purchased Yahoo!’s internet business in 2017.

a. On June 2, 2019, at 23:11 GMT, the user posted the question “Who wants to help me kill my parents?” The user followed up with the comment, “If you want to help me kill my parents call. I need them dead before my big plan.”

b. On June 2, 2019, at 23:05 GMT, the user posted the question, “Does anyone want to help me kill my parents?” The user followed up with the comment, “If you want to help me kill my parents you can give me a call. I will let you kill them before my big plan.”

c. On June 2, 2019, at 11:15 GMT, the user posted the question, “Does anyone know how I can contact the FBI or CIA?” The user followed up with the comment, “Or something, I’m 25 years old with autism spectrum disorder. I am planning to shoot up a Boston high school ether in September or October and I need their help sneaking in guns so my parents don’t see them. Yes I live with my parents.”

d. On May 31, 2019, at 22:49 GMT, the user posted the question, “Why do you bullies like making fun of autistic people like me?” The user followed up with the comment, “I’m a 25 year old with autistic spectrum disorder. I have been bullied all my life. So I’m planning a big event. I am going to shoot up a Boston high school ether September or October. i just can’t take it anymore.”

e. On May 31, 2019, at 11:15 GMT, the user posted the question, “Do any of you know how to make a bomb?” The user followed up with the comment, “I want to take the bomb some place to set it off.”

f. On May 12, 2019, at 14:30 GMT, the user posted the question, “Why do cameras want to control me and make me depressed and want to kill people?”

Interviews with Glidden

13. Because the threats on Twitter and Yahoo! Answers appeared to have been made by an individual in Maine, the investigation was assigned to FBI Special Agent Michael Verhar, who is assigned to the FBI's Bangor office. On June 2, 2019, Verhar spoke on the telephone with Waldoboro Police Sergeant Jamie Wilson, who had investigated Troy Glidden in connection with a 2014 incident in which Glidden had posted threatening comments on YouTube.² Wilson told Verhar that he was familiar with Glidden, and confirmed that Glidden lived with his parents. He said Glidden spent most of his time "trolling the internet." Wilson agreed to go to the Glidden residence and speak with Troy Glidden to find out whether he had made the comments on Twitter and Yahoo! Answers, and what had prompted him to make the comments.

14. On June 2, 2019, Wilson called Verhar and reported that he had made contact with Troy Glidden and his parents. Glidden admitted that he had made the online comments about being tired of being bullied, and wanting to shoot up a Boston school in September or October. He admitted that he was upset, and said it was primarily due to being bullied by other people online. Glidden said he wanted to go to the hospital to be evaluated, and his parents agreed with his decision. Wilson transported Glidden to Miles Memorial Hospital.

15. On June 13, 2019, Special Agent Verhar interviewed Glidden at his residence. Glidden's parents were also present for the interview. When asked about the online comments regarding shooting up a Boston high school, Glidden acknowledged making the comments, and said he did not know why he wrote them. He denied trying to obtain a firearm, or trying to obtain plans or materials to build a bomb. He said he had no plans to hurt others or himself. He claimed that he was feeling better than when he was admitted to the hospital over a week previously.

² Glidden told Wilson at the time that he did not want to hurt anyone and that he was just trying to get a reaction from people by posting the comments on YouTube. Charges ultimately were not filed.

Verhar told him that his online comments could be considered threats even if he was not taking active steps to carry out the threats, and admonished him not to make statements about shooting up schools or other public places. Verhar also advised him that if he continued to make similar online comments, law enforcement would need to find alternative methods of preventing him from continuing the behavior.

Additional Online Postings by Glidden

16. On August 14, 2019, the Boston Police Department received a report regarding an individual with the screen name “Troy” who been making comments on Yahoo! Answers about a previous threat he had made to shoot up a Boston high school.

17. A review of the Yahoo! Answers site revealed that “Troy” had indeed made a series of posts regarding his prior threat and his subsequent contacts with the FBI. They included the following posts:

a. “Will the FBI know its me if I change Yahoo Answer Accounts? I got into trouble with the FBI because I threaten to shoot up a Boston High School and I think their monitoring. Don’t call the FBI on me or anything. I’m just wondering.”

b. “Can someone please give me a ride down to Boston Massachusetts? I kneed a ride down to Boston Massachusetts without my parents knowing. I’m 25 years old by the way. I just have autism spectrum disorder. Hopefully the FBI don’t see this question.”

c. “How do I block the FBI from monitoring my computer? I need help blocking the FBI. I don’t want them to know what’s on my computer. Please don’t tell the FBI about this question. I don’t want to get into trouble again.”

d. “Who is your favorite serial killer?”

e. “Can I avoid jail if I have autism spectrum disorder?”

f. “Does anyone want to five me a ride down to Boston Massachusetts? I need a ride to Boston Massachusetts in September or October.”

g. “Why did the user Will have to report me to the FBI? Thanks to the user Will I spent over a week in a mental hospital. If you want to fight me, then fight me.”

18. Verizon Media also independently sent additional information to the Waldoboro Police Department regarding the user’s more recent posts on Yahoo! Answers. In addition to the posts described in the preceding paragraph, the information provided by Verizon showed that the user, who was associated with the Yahoo! account troyglidden723@yahoo.com, had made the following posts:

a. On August 19, 2019, at 23:17 GMT, the user posted the question, “How much money will you make if you sold a kidnapped kid to traffic?”

b. On August 19, 2019, at 22:10 GMT, the user posted the question, “What does it feel like to kidnap a kid?” The user followed up with the comment, “And what does the kid feel about being kidnapped.”

c. On August 19, 2019, at 01:34 GMT, the user posted the question, “Is there a police station next to any of the Boston high schools?”

d. On August 16, 2019, at 22:43 GMT, the user posted the question, “Do you know any thing about the Boston International High School?”

e. On August 16, 2019, at 22:32 GMT, the user posted the question, “Do any of you know anything about the East Boston High School?”

f. On August 16, 2019, at 20:43 GMT, the user posted the question, “Does Boston high schools have security?”

g. On August 13, 2019, at 17:08 GMT, the user posted the question, “How do I make a bomb?” The user followed up with the comment, “I want to watch a bomb go off in the woods like fireworks.”

h. On August 12, 2019, at 02:14 GMT, the user posted the question, “Who wants to help me shoot up a Boston high school?” The user followed up with the comment, “Just give me a ride and some guns. Or you can shoot up a Boston high school yourself and give me some credit.”

19. Verizon also reported that the user-provided name on the Yahoo! account was “Troy Glidden,” and that the account was created on July 15, 2019, from an IP address that geo-located to the area around Boothbay Harbor. The user provided the same date of birth in 1993 as the actual date of birth for Troy Glidden. The Yahoo! account was deactivated on August 20, 2019, for a violation of Yahoo!’s Terms of Service.

Interstate Commerce

20. When Troy Glidden posted to Twitter and to the Yahoo! Answers website, the information he posted was transmitted via the internet from Maine to servers operated by Yahoo! and Twitter. I know that Glidden’s threatening communications traveled between states because an individual in Kentucky contacted the FBI regarding Glidden’s posts on Twitter, and an individual in Illinois contacted the FBI about his posts on Yahoo! Answers. I also know from conversations with the United States Attorney’s Office for the District of Maine that courts have concluded that transmission of information by means of the internet is equivalent to moving the information across state lines, and therefore constitutes transmission in interstate commerce.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

21. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

22. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has

been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information

about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

c. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence

and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

d. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

e. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

g. I know that when an individual uses a computer to make interstate online threats the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the offense.

24. *Outbuildings and motor vehicles.* Based on my training and experience I know that devices that could be used to commit the offense under investigation are by their very nature portable. These include laptop computers, tablets and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such items in multiple locations within their premises, including in outbuildings and motor vehicles. Specific to this investigation, on August 28, 2019, another investigator and I drove by the Premises and observed that there was a camper parked next to the residence. It appeared that the camper may have been occupied recently. In addition, we observed a shed next to the camper and in close proximity to the residence. For these reasons, the warrant for which I am applying will permit investigators

executing the warrant to search all outbuildings, recreational vehicles and motor vehicles located on the Premises.

25. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. **The time required for an examination.** As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. **Technical requirements.** Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not

be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. **Variety of forms of electronic media.** Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

27. Because several people share the Premises as a residence, it is possible that the Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

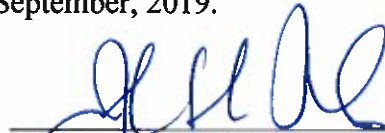
28. Based on the foregoing, I believe that there is probable cause to believe that violations of 18 U.S.C. § 875(c) have occurred, and that the evidence and instrumentalities of this offense, more fully described in Attachment B, are located at the location described in Attachment A. I respectfully request that the Court issue a search warrant for the location described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

I declare that the foregoing is true and correct.



Joshua Borges
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me this 3rd day of September, 2019.



John H. Rich III
United States Magistrate Judge
District of Maine